BULLETIN (SB19-336)
VULNERABILITY SUMMARY FOR THE WEEK OF NOVEMBER 25, 2019

Bulletin (SB19-336)
Vulnerability Summary for the Week of November 25, 2019

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.

Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -

Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .
The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
chicken -- chicken	Buffer overflow in CHICKEN 4.9.0 and 4.9.0.1 may allow remote attackers to execute arbitrary code via the 'select' function.	2019-11-22	7.5	CVE-2014-6310
google -- chrome	Out of bounds memory access in JavaScript in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	7.5	CVE-2019-5866
red_hat -- redhat-upgrade-tool	redhat-upgrade-tool: Does not check GPG signatures when upgrading versions	2019-11-22	10	CVE-2014-3585 REDHAT REDHAT

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gael -- q-pulse	Cross-site scripting (XSS) vulnerability in ui/common/managedlistdialog.aspx in Gael Q-Pulse 0.6 and earlier.	2019-11-22	4.3	CVE-2014-1238 MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 12.4. It has Insecure Permissions.	2019-11-26	4	CVE-2019-18447 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition through 12.4. It has Insecure Permissions (issue 2 of 4).	2019-11-26	4	CVE-2019-18458 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 11.3 through 12.4 when moving an issue to a public project from a private one. It has Insecure Permissions.	2019-11-26	5	CVE-2019-18452 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 11.6 through 12.4 in the add comments via email feature. It has Insecure Permissions.	2019-11-26	4	CVE-2019-18453 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 12.4 in the Project labels feature. It has Insecure Permissions.	2019-11-26	4	CVE-2019-18450 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 12.4. It has Incorrect Access Control.	2019-11-26	4	CVE-2019-18448 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 8.15 through 12.4 in the Comments Search feature provided by the Elasticsearch integration. It has Incorrect Access Control.	2019-11-26	5	CVE-2019-18460 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 11.8 through 12.4 when handling Security tokens.. It has Insecure Permissions.	2019-11-26	6.5	CVE-2019-18457 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 10.7.4 through 12.4 in the InternalRedirect filtering feature. It has an Open Redirect.	2019-11-26	5.8	CVE-2019-18451 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 10.5 through 12.4 in link validation for RDoc wiki pages feature. It has XSS.	2019-11-26	4.3	CVE-2019-18454 MISC MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 8.15 through 12.4. It has Insecure Permissions (issue 1 of 2).	2019-11-26	5.5	CVE-2019-18446 CONFIRM MISC
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 11 through 12.4 when building Nested GraphQL queries. It has a large or infinite loop.	2019-11-26	5	CVE-2019-18455 MISC MISC
google -- chrome	Insufficient validation of untrusted input in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13710 MISC MISC
google -- chrome	Insufficient policy enforcement in the Omnibox in Google Chrome on Android prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13703 MISC MISC
google -- chrome	Insufficient policy enforcement in reader mode in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13692 MISC MISC
google -- chrome	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-11-25	5	CVE-2019-13711 MISC MISC
google -- chrome	Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13695 MISC MISC
google -- chrome	Insufficient policy enforcement in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13704 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in navigation in Google Chrome on iOS prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13708 MISC MISC
google -- chrome	Insufficient validation of untrusted input in Color Enhancer extension in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to inject CSS into an HTML page via a crafted URL.	2019-11-25	4.3	CVE-2019-13714 MISC MISC
google -- chrome	Insufficient validation of untrusted input in intents in Google Chrome on Android prior to 78.0.3904.70 allowed a local attacker to leak files via a crafted application.	2019-11-25	4.3	CVE-2019-13707 MISC MISC
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-11-25	4.3	CVE-2019-13715 MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 78.0.3904.70 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension.	2019-11-25	4.3	CVE-2019-13705 MISC MISC
google -- chrome	Out of bounds read in Skia in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-11-25	5.8	CVE-2019-5849 MISC MISC
google -- chrome	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13717 MISC MISC
google -- chrome	Insufficient policy enforcement in service workers in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13716 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13687 MISC MISC
google -- chrome	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13719 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient data validation in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-11-25	4.3	CVE-2019-13718 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 76.0.3809.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	4.3	CVE-2019-5869 MISC MISC
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	4.3	CVE-2019-5847 MISC MISC
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-11-25	4.3	CVE-2019-5852 MISC MISC
google -- chrome	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13713 MISC MISC
google -- chrome	Use after free in PDFium in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-11-25	4.3	CVE-2019-5868 MISC MISC
google -- chrome	Use after free in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-11-25	4.3	CVE-2019-5860 MISC MISC
google -- chrome	Use after free in Mojo in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	4.3	CVE-2019-5872 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13688 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 75.0.3770.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	4.3	CVE-2019-5842 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13709 MISC MISC
google -- chrome	Use after free in offline mode in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13686 MISC MISC
google -- chrome	Insufficient policy enforcement in performance APIs in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13697 MISC MISC
google -- chrome	Use after free in media in Google Chrome on Android prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-5876 MISC MISC
google -- chrome	Use after free in WebAudio in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-5851 MISC MISC
google -- chrome	Use after free in PDFium in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13721 MISC MISC
google -- chrome	Use after free in media in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13699 MISC MISC
google -- chrome	Out of bounds memory access in the gamepad API in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13700 MISC MISC
google -- chrome	Inappropriate implementation in installer in Google Chrome on Windows prior to 78.0.3904.70 allowed a local attacker to perform privilege escalation via a crafted executable.	2019-11-25	6.8	CVE-2019-13702 MISC MISC
google -- chrome	Out of bounds memory access in PDFium in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-11-25	6.8	CVE-2019-13706 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13720 MISC MISC
google -- chrome	Incorrect font handling in autofill in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-11-25	4.3	CVE-2019-5848 MISC MISC
google -- chrome	Out of bounds memory access in WebBluetooth in Google Chrome prior to 78.0.3904.108 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13724 MISC MISC
google -- chrome	Use after free in offline mode in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-11-25	6.8	CVE-2019-5850 MISC MISC
google -- chrome	Use after free in IndexedDB in Google Chrome prior to 77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13693 MISC MISC
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-5853 MISC MISC
google -- chrome	Insufficient validation of untrusted input in navigation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13691 MISC MISC
google -- chrome	Incorrect implementation in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13701 MISC MISC
google -- chrome	Integer overflow in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-11-25	6.8	CVE-2019-5854 MISC MISC
google -- chrome	Use after free in media in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2019-11-25	6.8	CVE-2019-5870 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Out of bounds memory access in JavaScript in Google Chrome prior to 73.0.3683.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13698 MISC MISC
google -- chrome	Use after free in V8 in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-5878 MISC MISC
google -- chrome	Use after free in JavaScript in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13696 MISC MISC
google -- chrome	Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-11-25	4.3	CVE-2019-13683 MISC MISC
google -- chrome	Use after free in WebRTC in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13694 MISC MISC
google -- chrome	Use after free in sharing view in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-11-25	6.8	CVE-2019-13685 MISC MISC
ibm -- smartcloud_analytics	IBM SmartCloud Analytics 1.3.1 through 1.3.5 is vulnerable to possible host header injection attack that could lead to HTTP cache poisoning or firewall bypass. IBM X-Force ID: 159187.	2019-11-22	4.9	CVE-2019-4216 XF CONFIRM
ibm -- smartcloud_analytics	IBM SmartCloud Analytics 1.3.1 through 1.3.5 does not set the secure attribute on authorization tokens or session cookies. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 159185.	2019-11-22	4.3	CVE-2019-4214 XF CONFIRM
ibm -- smartcloud_analytics	IBM SmartCloud Analytics 1.3.1 through 1.3.5 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 159186.	2019-11-22	4.3	CVE-2019-4215 XF CONFIRM
openstack -- designate	Designate does not enforce the DNS protocol limit concerning record set sizes	2019-11-22	4	CVE-2015-5694 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC MISC
ovirt -- ovirt	oVirt users with MANIPULATE_STORAGE_DOMAIN permissions can attach a storage domain to any data-center	2019-11-22	4	CVE-2015-1780 MISC MISC
pagekit -- pagekit	A CSRF vulnerability in Pagekit 1.0.17 allows an attacker to upload an arbitrary file by removing the CSRF token from a request.	2019-11-22	6.8	CVE-2019-19013 MISC
plow -- plow	plow has local buffer overflow vulnerability	2019-11-22	4.6	CVE-2012-3407 MISC MISC MISC
postfixadmin -- postfixadmin	PostfixAdmin 2.3.4 has multiple XSS vulnerabilities	2019-11-22	4.3	CVE-2012-0812 MISC MISC MISC MISC MISC MISC MISC
zte -- zxcdn_iamweb	The version V6.01.03.01 of ZTE ZXCDN IAMWEB product is impacted by a code injection vulnerability. An attacker could exploit the vulnerability to inject malicious code into the management page, resulting in users? information leakage.	2019-11-22	6.5	CVE-2019-3427 CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-11-25	2.6	CVE-2019-13684 MISC MISC
ibm -- smartcloud_analytics	IBM SmartCloud Analytics 1.3.1 through 1.3.5 allows unauthorized disclosure of information like accessing solrconfig.xml and could allow an attacker to perform disruptive administrator tasks. IBM X-Force ID: 159517.	2019-11-22	3.6	CVE-2019-4243 XF CONFIRM
videolan -- libbluray	libbluray MountManager class has a time-of-check time-of-use (TOCTOU) race when expanding JAR files	2019-11-22	3.3	CVE-2015-7810